EXHIBIT 4

to T-Mobile's Responsive Claim Construction Brief

GSM SYSTEM ENGINEERING

MOBILE COMMUNICATIONS SERIES

ASHA MEHROTRA

Artech House Publishers

GSM System Engineering

Asha Mehrotra

Artech House, Inc.
Boston • London

Library of Congress Cataloging-in-Publication Data
Mehrotra, Asha.
GSM System Engineering / Asha Mehrotra.
p. cm.
Includes bibliographical references and index.
ISBN 0-89006-860-7 (alk. paper)
1.Global system for mobile communications. I. Title.
TK5103.483.M45 1996
621.3845'6—dc21 97-4029
CIP

British Library Cataloguing in Publication Data
Mehrotra, Asha
GSM System Engineering
1. Cellular radio 2. Mobile communication systems.
I. Title
621.3'8456

ISBN 0-89006-860-7

Cover design by Jennifer Makower.

685 Canton Street
Norwood, MA 02062

International Standard Book Number: 0-89006-860-7
Library of Congress Catalog Card Number: 97-4029

10 9 8 7 6 5 4 3 2

CHAPTER 2

GSM ARCHITECTURE

2.1 INTRODUCTION

A GSM system is basically designed as a combination of three major subsystems: the network subsystem, the radio subsystem, and the operation support subsystem. In order to ensure that network operators will have several sources of cellular infrastructure equipment, GSM decided to specify not only the air interface, but also the main interfaces that identify different parts. There are three dominant interfaces, namely, an interface between MSC and the *Base Station Controller* (BSC), an A-bis interface between BSC and the *Base Transceiver Station* (BTS), and an Um interface between the BTS and MS. These three interfaces are shown in Figure 1.6.

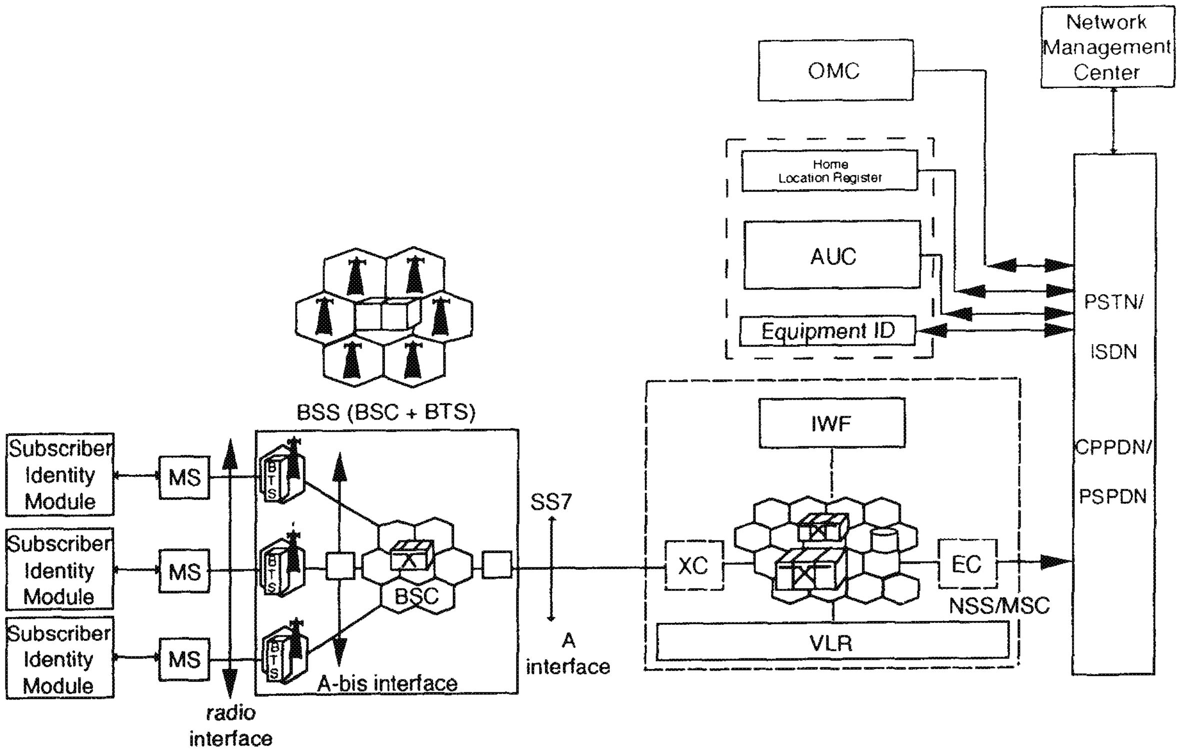
The network subsystem includes the equipment and functions related to end-to-end calls, management of subscribers, mobility, and interface with the fixed PSTN. In particular, the switching subsystem consists of MSCs, *Visitor Location Register* (VLR), *Home Location Register* (HLR), *Authentication Center* (AUC), and *Equipment Identity Register* (EIR). The MSC provides call setup, routing, and handover between BSCs in its own area and to/from other MSC; an interface to the fixed PSTN; and other functions such as billing. The HLR is a centralized database of all subscribers registered in a PLMN. There may be more than one HLR in PLMN, but the individual subscriber has entry to only one of them. The VLR is a database

of all mobile, currently roaming in the MSC's area of control. As soon as an MS roams into a new MSC area, the VLR connected to that MSC will request data about the MS from the HLR. At the same time, the HLR will be informed as to which MSC area the MS resides. If, at a later time, MS wants to make a call, the VLR will have all the information needed for the call setup without having to interrogate the HLR each time. Thus, VLR in one sense is a distributed HLR. VLR also contains more exact information about the mobile location. The AUC is connected to the HLR. The function of the AUC is to provide HLR with authentication parameters and ciphering keys that are used for security purposes. The EIR is the database where the *International Mobile Equipment Identity* (IMEI) numbers for all registered mobile equipment are stored.

Some other components of the network are Echo Canceler, which reduces the annoying effect caused by the mobile network when connected to a PSTN circuit; and the network *Interworking Function* (IWF), which is the interface between MSC and other networks such as PSTN and ISDN.

The radio subsystem includes the equipment and functions related to the management of the connections on the radio path, including the management of handovers. It mainly consists of a BSC, BTS, and the MS. MS is traditionally listed as a part of the radio subsystem even though it is always one end of the conversational path and holds dialogues with the network subsystem for the management of its mobility. The MS includes both the capabilities of network termination and user termination. The GSM system is realized as a network of radio cells, which together provide complete coverage of the service area. Each cell has a BTS with several transceivers. A group of BTSs are controlled by one BSC. There are various configurations of BSC-BTS. Some configurations are best suited for high traffic, and some are meant to serve moderate-to-low traffic areas. A BSC controls such functions as handover and power control. BSS and BTS together are known as a BSS, which is viewed by the MSC through a single interface as being the entity responsible for communication with MSs in a certain area. A BSS is associated with the radio channel management, transmission functions, radio link control, and quality assessment and preparation for handover. BSS ensures the coverage of N cells, where N can be one or more.

The *Operational and Maintenance Center* (OMC) subsystem includes the operation and maintenance of GSM equipment and supports the operator network interface. It is connected to all equipment in the switching system and to the BSC. OMC performs GSM's administrative functions (for example, billing) within a country. One of the OMC's most important functions is the maintenance of the country's HLR. Depending upon the network size, each country may have more than one OMC. The global and centralized management of the network is provided by the Network Management Center, while the OMC is responsible for the regional management of the network. Two typical GSM architectures are shown in Figures 2.1(a, b).



CSPDN: Circuit Switched Public Data Network
PSPDN: Packet Switched Public Data Network
XC: Trancoder

(a)

Figure 2.1 (a) Typical GSM architecture; (b) GSM system model.

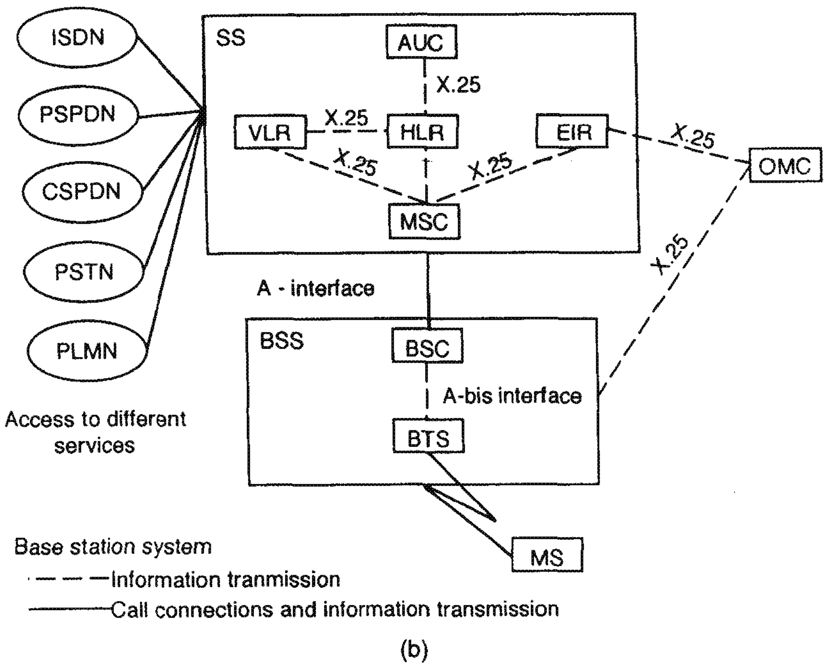


Figure 2.1 (continued).

In view of this introduction, the objective of this chapter is to discuss the functions of various network subsystems, radio subsystems, operational and maintenance subsystems, and billing subsystems. Before we take up the study of these subsystems let us first discuss the layout of the GSM network.

2.2 GSM NETWORK STRUCTURE

Every telephone network needs a well-designed structure in order to route incoming calls to the correct exchange and finally to the called subscriber. In a mobile network, this structure is of great importance because of the mobility of all its subscribers [1–4]. In the GSM system, the network is divided into the following partitioned areas.

- GSM service area;
- PLMN service area;
- MSC service area;
- *Location area* (LA);
- Cells.

The GSM service area is the total area served by the combination of all member countries where a mobile can be serviced. The next level is the PLMN service area. There can be several within a country, based on its size. The links between a GSM/PLMN network and other PSTN, ISDN, or PLMN networks will be on the level of international or national transit exchanges. All incoming calls for a GSM/PLMN network will be routed to a Gateway MSC. A Gateway MSC works as an incoming transit exchange for the GSM/PLMN. In a GSM/PLMN network, all mobile-terminated calls will be routed to a Gateway MSC. Call connections between PLMNs, or to fixed networks, must be routed through certain designated MSCs called a gateway MSC. The gateway MSC contains the interworking functions to make these connections. They also route incoming calls to the proper MSC within the network. The next level of division is the MSC/VLR service area. In one PLMN there can be several MSC/VLR service areas. MSC/VLR is a sole controller of calls within its jurisdiction. In order to route a call to a mobile subscriber, the path through the network links to the MSC in the MSC area where the subscriber is currently located. The mobile location can be uniquely identified since the MS is registered in a VLR, which is generally associated with an MSC. The PLMN and MSC/VLR service areas are shown in Figures 2.2(a,b).

The next division level is that of the LAs within a MSC/VLR combination. There are several LAs within one MSC/VLR combination. A LA is a part of the MSC/VLR service area in which a MS may move freely without updating location information to the MSC/VLR exchange that controls the LA. Within a LA a paging message is broadcast in order to find the called mobile subscriber. The LA can be identified by the system using the *Location Area Identity* (LAI). The LA is used by the GSM system to search for a subscriber in active state.

Lastly, a LA is divided into many cells. A cell is an identity served by one BTS. The MS distinguishes between cells using the *Base Station Identification Code* (BSIC) that the cell site broadcasts over the air. The division of LA into many cells is shown in Figure 2.2(c). The overall relationship between cells, LA, MSC service area, PLMN service area, and GSM service area is shown in Figure 2.2(d). Coding for LA is shown in Figure 2.2(e).

2.2.1 Cell Layout and Frequency Planning

From the system design point-of-view we consider the cell to be hexagonal, but in real life it happens to be irregular in shape and size due to uneven propagation in different radials. At the cell boundary, the power received from the BTS should be adequate for reception with an acceptable *bit error rate* (BER). In general, this can be achieved at most locations from more than one BTS, leading to an overlap of the actual cell coverage. The cell boundaries are the line of equal power from two adjacent *base stations* (BS); therefore, the cell sizes will vary as the BTS power is

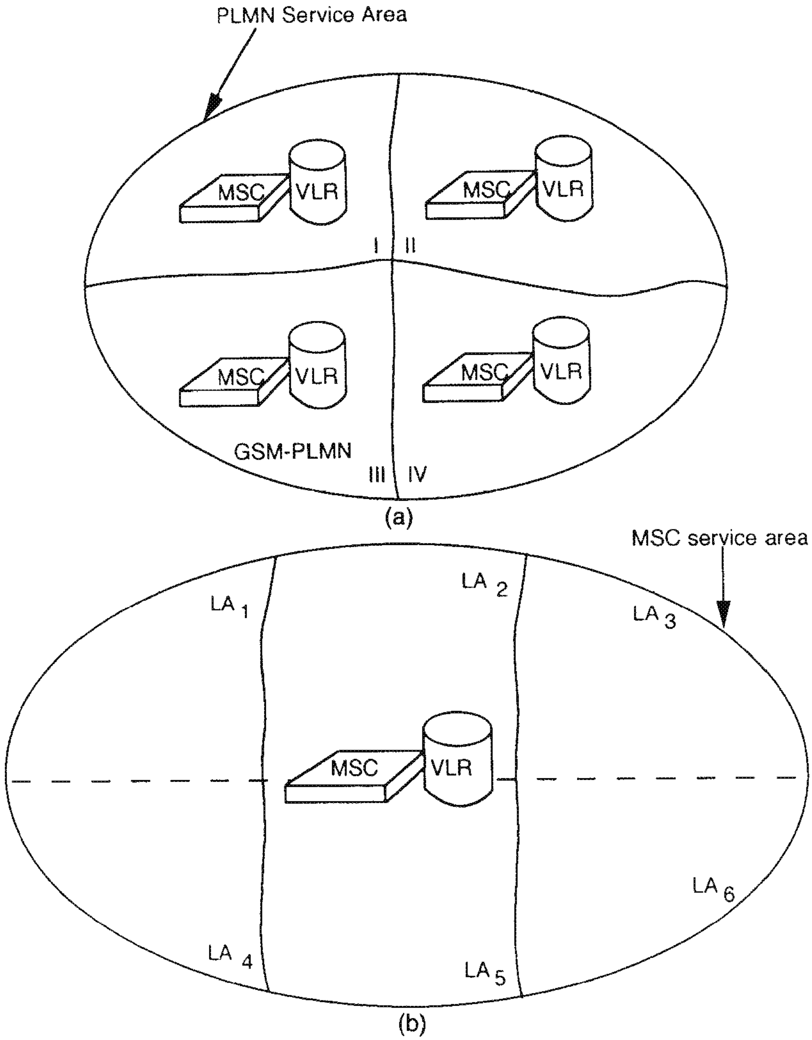
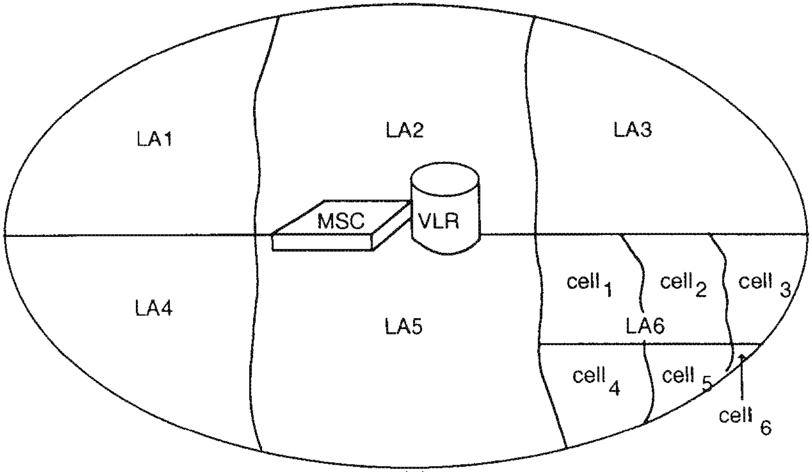


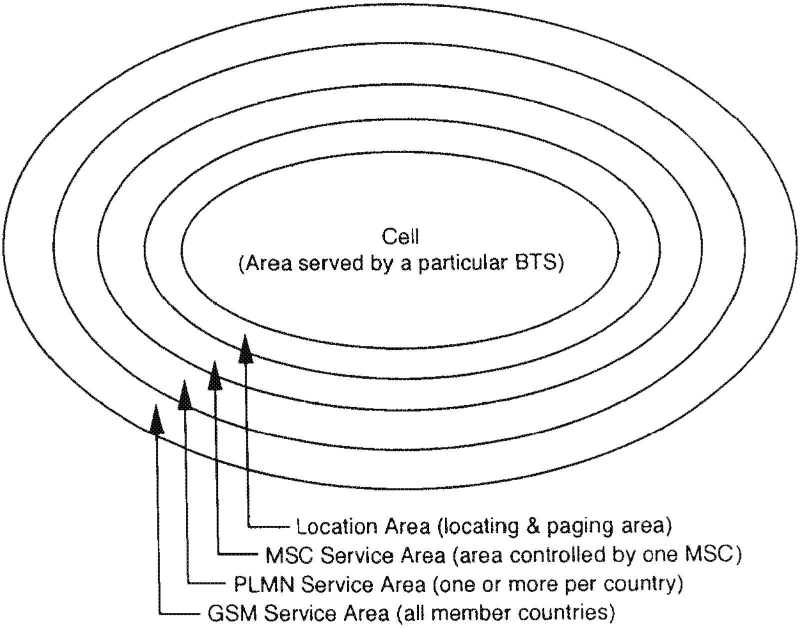
Figure 2.2 (a) PLMN service areas I to IV; the division of a MSC/VLR service area into (b) LAs and (c) cells; (d) relation between areas in GSM; (e) LA coding.

adjusted. The layout of a typical MSC/VLR LA with overlapping cell sites is shown in Figure 2.3(a).

GSM has chosen the four-cell repeat pattern for the frequency reuse cell sets. In most cases, each cell is divided into 120-deg sectors, with three base transceiver subsystems in each cell. Each base transceiver subsystem has a 120-deg antenna. In some low-traffic areas, an omnidirectional setup can be used.

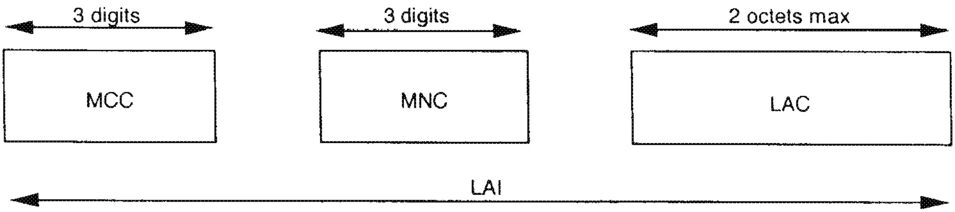


(c)



(d)

Figure 2.2 (continued).



MCC - Mobile Country Code: identifies the country in which the GSM PLMN is located. Thus the value of the MCC is the same as the 3 digit MCC contained in the IMSI of any subscriber belonging to the country presently visited by the mobile station.

MNC - Mobile Network Code: is a code identifying the GSM PLMN in that country. Thus the value of the MNC is the same as the 3 digit MNC contained in the IMSI of any subscriber belonging to the country presently visited by the mobile station.

LAC - Location Area Code: it is flexible length code, up to 2 octets maximum, identifying a location area within a GSM PLMN.

(e)

Figure 2.2 (continued).

With a four-cell repeat pattern and three-sectored antenna per cell site, there are 12 sectors (called cells in a GSM system) in which the total number of 124 channels needs to be divided, assuming that the full spectrum is available from the operator of the system. The four-cell coverage pattern is shown in Figure 2.3(b). For optimum frequency separation, within the same sector (cell), assign to the Kth sector (cell) K, $K + N$, $K + 2N$, . . . , $K + nN$, where n is an integer such that $(124 - nN)/N < 1$. Thus, in this case where $N = 12$ for the first sector, the assigned channels are 1, 13, 25, 37, . . . , 121. Since there are 12 sectors (called cells in GSM) per repeat pattern, each sector (cell) then gets approximately one-twelfth of the available frequencies. The frequency assignment for this example is shown in Table 2.1. Here the pattern of cell frequency assignments (A, B, . . .) is repeated so that frequencies are reused with an acceptably small level of cochannel interference.

2.3 MOBILE STATION

The MS includes radio equipment and the *man machine interface* (MMI) that a subscriber needs in order to access the services provided by the GSM PLMN. MSs can be installed in vehicles or can be portable or handheld stations. The MS may include provisions for data communication as well as voice. A mobile transmits and receives messages to and from the GSM system over the air interface to establish and continue connections through the system [1,5–8].

CHAPTER 3

TIME AND FREQUENCY AXIS REPRESENTATION

3.1 INTRODUCTION

GSM was first devised as a cellular system specific to the 900-MHz band, called "the primary band." This primary band includes two subbands of 25 MHz each, 890 MHz to 915 MHz and 935 MHz to 960 MHz. However, the whole primary band does not have to be used for GSM in a given country, especially at the start of the system when the traffic may not justify the allocation of the whole spectrum. In general, since most countries have several operators, an operator is rarely given more than a portion of this band. On the other hand, every MS must be able to use the full band so as not to impose constraints upon roaming users. Thus, the GSM PLMN has allocated 124 duplex carrier frequencies over the following bands of operation.

- Uplink: 890 MHz to 915 MHz (MS transmit, BTS receive);
- Downlink: 935 MHz to 960 MHz (BTS transmit, MS receive);
- Carrier spacing 200 kHz.

The time and frequency domain layout of a GSM system is shown in Figure 3.1. Since there are a total of eight channels per carrier, the total number of channels in

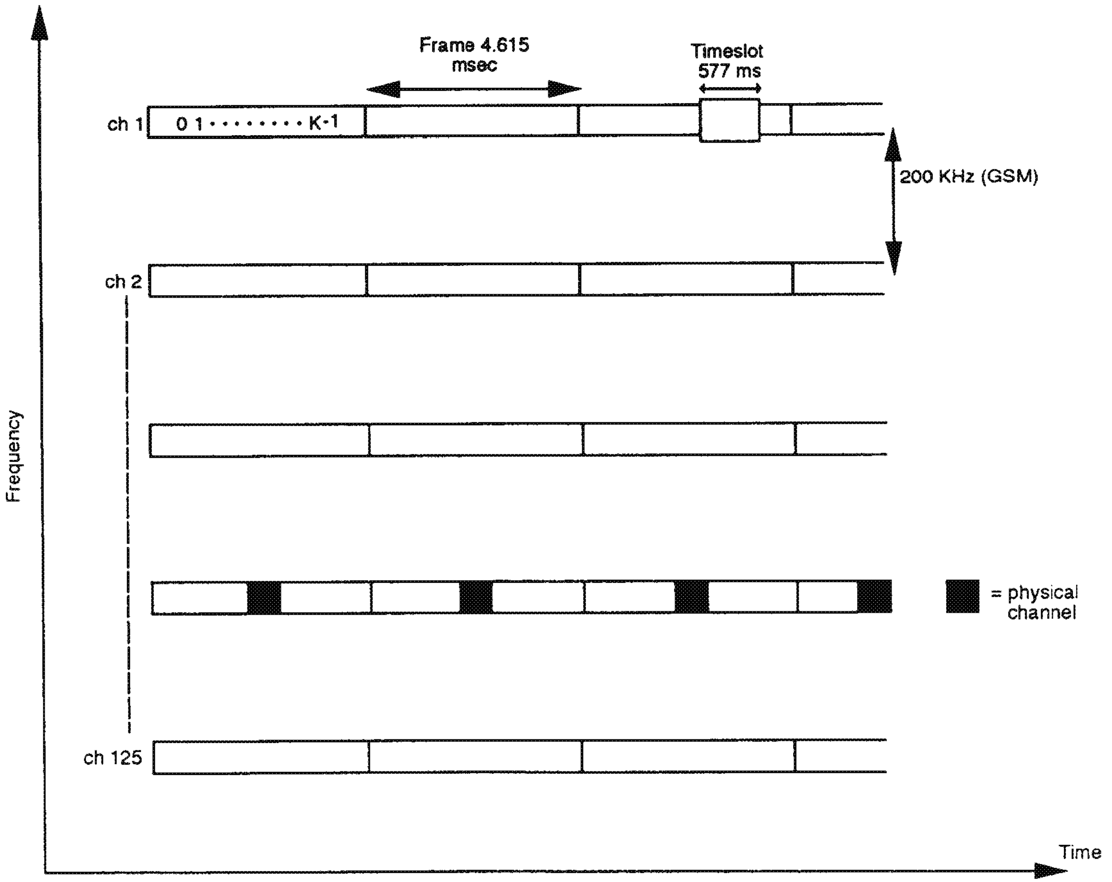


Figure 3.1 Time and frequency domain access for cellular radio [1].

a GSM system are, therefore, 125 × 8 = 1,000 channels. In actuality, only 124 carriers are used. There is a total of eight bursts during a frame cycle, which is defined as the information format during one timeslot on the TDMA channel; that is, with regular time intervals (every eighth timeslot on a TDMA channel, the user transmits or receives his information), we send a burst of information (either speech or data). Thus, a burst is considered as a period of RF carrier that is modulated by a data stream. A burst therefore represents the physical content of a timeslot. This burst period (15/26 ms) is shown in Figure 3.2.

In 1990, at the request of the United Kingdom, a second frequency band was specified. This band includes two frequency ranges: 1710 MHz to 1785 MHz and 1805 MHz to 1880 MHz; that is, twice 75 MHz and three times as much as the primary 900 MHz. MSs using this band will have different constraints from those using the primary band. Using the same ME for roaming between the two variants of the system, GSM 900 and DCS 1800, although not ruled out, is difficult to envision. Another extension of the primary band is also foreseen. It will consist of a band that is directly "below" the primary band. For instance, an 8-MHz extension would raise the 900-MHz bands from 882 MHz to 915 MHz and 927 MHz to 960 MHz, that is, twice 33 MHz.

The central frequencies of the channel slots are spread evenly at every 200-kHz interval within these bands, starting 200 kHz away from the band borders. Therefore, 124 different frequency slots are defined in 25 MHz, and 374 in 75 MHz. The modulation spectrum is somewhat wider than 200 kHz, resulting in some level of interference on adjacent frequency slots. This is a nuisance at least near the band borders, since this interference could disturb non-GSM applications in adjacent bands. The border frequencies are usually avoided. The normal practice is not to use the frequency slots at the border (those numbered 0 to 4) except when a special agreement has been reached with the users of the adjacent band. As a consequence,

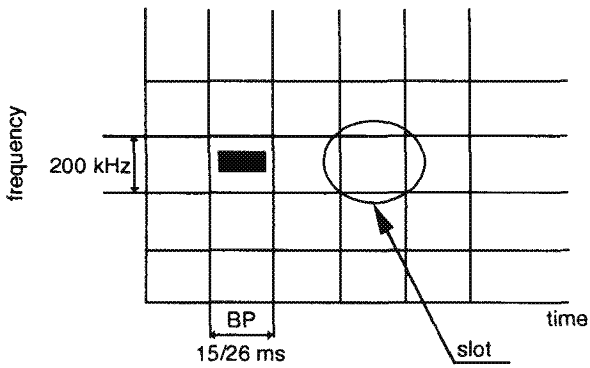


Figure 3.2 A slot in the time and frequency domain.

the number of frequency slots that can be used in 25 MHz can be limited to 122, though in most systems 124 channels have been used.

In view of this discussion, we shall examine the following concepts in this chapter. Section 3.2 provides the time domain representation of the GSM system, including details of logical channels, the physical layer description of different types of bursts, and how the speech and control channels are organized within the system. In Section 3.3 we shall discuss the frequency domain description of the system followed by some operational concepts in Section 3.4.

3.2 TIME DOMAIN REPRESENTATION

As mentioned in Section 3.1, the GSM system has a total available bandwidth of 25 MHz divided among 124 channels of 200 kHz each (as shown in Figure 3.1). It should be noted that there are a total of 125 channels, out of which the lowest channel is not used as it may interfere with other nearby non-GSM systems. Each of these 124 channels operates at different carrier frequencies. An individual channel is time division multiple accessed by users at different locations within a cell site. The frame duration is 4.615 ms divided among eight timeslots. Each of these timeslots is a physical channel occupied by an individual user. Each timeslot, or physical channel, carries control and traffic data in a burst form. The time duration of an individual channel is 3/5200 sec or 0.577 ms. At the BTS, TDMA frames on all radio frequency channels, in the downlink as well as on the uplink, are aligned. However, the start of an uplink TDMA frame is delayed with respect to downlink by a fixed period of three timeslots. Staggering TDMA frames allows the same *timeslot number* (TN) to be used in both the down and uplinks while avoiding the requirement for mobile to transmit and receive simultaneously. The TN within a frame is numbered from 0 to 7, and each TN can be referenced by a unique TN. Higher order frames, called multiframe, consist of 26 frames and have a duration of 120 ms (26×4.615 ms). This multiframe consists of 26 TDMA frames and carries a *traffic channel* (TCH), *slow associated control channel* (SACCH), and *fast associated control channel* (FACCH). Similarly, a 51-frame multiframe has a duration of 235.365 ms (51×4.615 ms). One superframe consists of 51 traffic multiframes or 26 control multiframes and consists of 51×26 TDMA frames with a total duration of 6.12 sec (51×120 ms). A 26 TDMA frame multiframe supports traffic and associated control channels, and a 51 TDMA frame multiframe supports *Broadcast Common Control* (BCC) and Stand Alone Dedicated Control Channels. The highest order frame is called a hyperframe and consists of 2,048 superframes, or 2,715,648 frames ($2048 \times 51 \times 26$). The frame number is cyclic and has a range from 0 to FN_MAX, where FN_MAX = $(2048 \times 51 \times 26) - 1 = 2{,}715{,}647$. The frame number is incremented at the end of each frame. The time duration of the hyperframe is 3 hrs, 28 min, and 52.76 sec ($2{,}715{,}648 \times 4.615$ ms). This long period

of a hyperframe is required to support encryption with high security. To organize the information transmitted on each carrier, GSM defines several time intervals ranging from 0.9 μs (quarter of one bit in the guard interval of the basic frame to be discussed in Section 3.2.4) to a hyperframe interval of over three hours. Details of frame, multiframe, superframe, and hyperframe are provided in Figure 3.3. As seen from the figure, the cycle of a multiframe and superframe is different for speech and control channels. It is not by accident that the control channel multiframe is not a direct multiple of the TCH multiframe. It can be seen that any frame number will only occur simultaneously in both multiframes every 1,326 frames (26×51). This arrangement means that the timing of the TCH multiframe is always moving in relation to that of the control channel multiframe, and this enables a receiver to receive and decode all the control channels along with TCH. If two multiframes were exact multiples of each other, then the control channel timeslot would be permanently "masked" by the TCH timeslot activity. This changing relationship is particularly important, for example, to a mobile unit that needs to be able to monitor and report RSSIs of up to six target cells (it needs to be able to see all the BCCHs of surrounding cells in order to do this).

3.2.1 Logical Channels

A great variety of information must be transmitted between the BTS and the MS, specifically, user data and control signaling. Depending on the kind of information transmitted, we refer to different logical channels. These logical channels are mapped onto the physical channels (slots). Digital speech is sent on a logical channel, named TCH, which during the transmission can be allocated a certain physical channel, say channel *Timeslot 7* (TS 7). In a GSM system no RF carrier and no slot is dedicated a priori to the exclusive use of anything. In other words, just about any slot of any RF carrier can be used for a number of different uses. Channelization is accomplished by the data communications notion of virtual circuits or logical channels. Logical channels are divided into the two categories, TCHs and control channels. We shall now provide details of these logical channels.

3.2.2 Logical TCHs

TCHs are intended to carry either encoded speech or user data both in the up and downlink directions in a point-to-point communication. There are two types of TCHs that are differentiated by their traffic rates and are defined as follows.

A *full rate TCH* (TCH/F), B_m , carries information (encoded speech or data) at a gross rate of 22.8 Kbps. The raw data rate for each TCH is 13 Kbps for speech and 12 Kbps, 6 Kbps, and 3.6 Kbps for data. The actual user data rates are

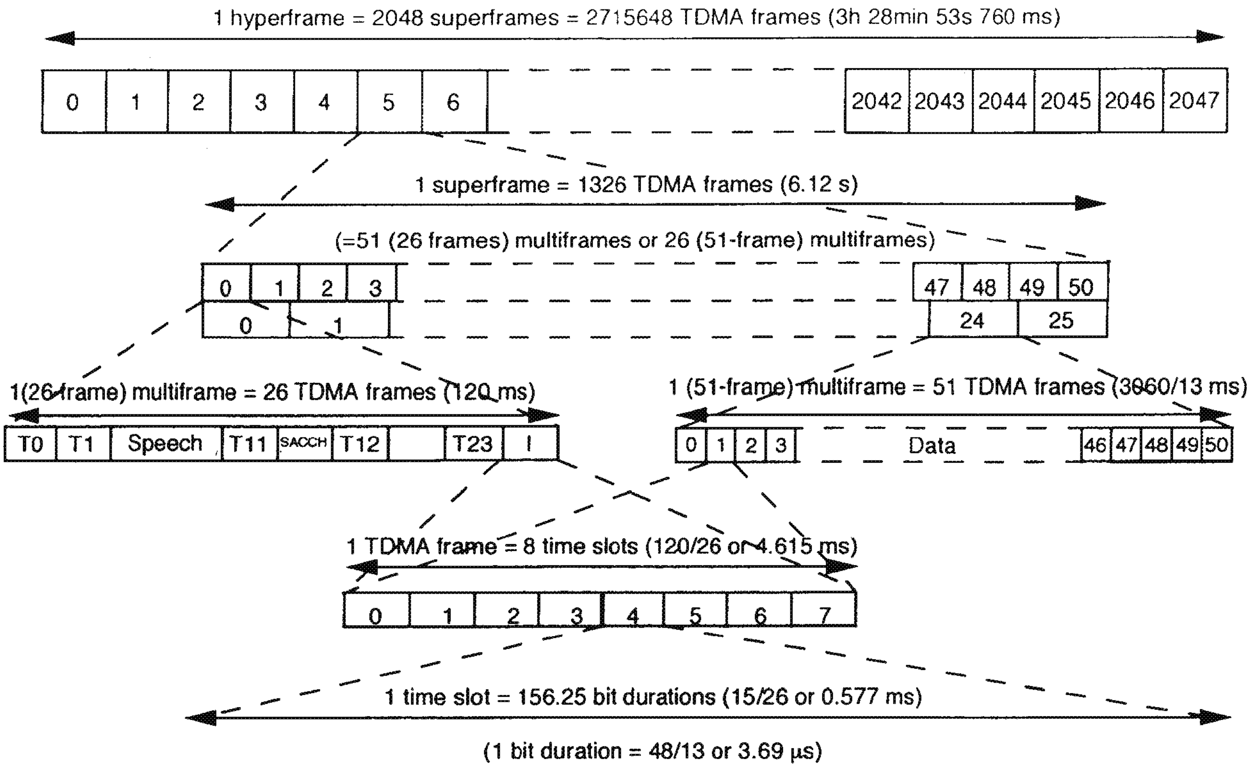


Figure 3.3 Frame, multiframe, superframe, and hyperframe for a GSM network.

9.6 Kbps, 4.8 Kbps, and 2.4 Kbps, which are padded to bring up the rates to 12 Kbps, 6 Kbps, and 3.6 Kbps.

A half rate TCH (TCH/H), L_m, carries information (encoded speech or data) at half of the full rate channel or at the gross rate of 11.4 Kbps. The user data rate associated with the half rate TCH are as follows. 4.8 Kbps and 2.4 Kbps. The allowed combinations of user data rate with full and half rate speech are as follows.

- Full rate speech (TCH/F);
- Half rate speech (TCH/H);
- 9.6 Kbps full rate data (TCH/F9.6);
- 4.8 Kbps full rate data (TCH/F4.8);
- 2.4 Kbps full rate data (TCH/F2.4);
- 4.8 Kbps half rate data (TCH/H4.8);
- 2.4 Kbps half rate data (TCH/H2.4).

3.2.3 Logical Control Channels

Most of the user services offered by GSM rely on the four transmission modes (single speech and three data modes). Control channels are intended to carry signaling or synchronization data. Three kinds have been defined below.

- *Broadcast Control Channel* (BCCH);
- *Common Control Channel* (CCCH);
- *Dedicated Control Channel* (DCCH).

Figure 3.4 shows details of different logical channels. The BCCH is a point-to-multipoint unidirectional control channel from the fixed subsystem to the MS that is intended to broadcast a variety of information to MSs, including information necessary for the MS to register in the system. The BCCH includes a *Frequency Correction Channel* (FCCH), which is used to allow an MS to accurately tune to a BS, and the *Synchronization Channel* (SCH), which is used to provide TDMA frame-oriented synchronization data to a MS. When mobile recovers both FCCH and SCH signals, we consider the synchronization to be complete.

A CCCH is a point-to-multipoint (bidirectional control channel) channel that is primarily intended to carry signaling information necessary for access management functions (e.g., allocation of dedicated control channels). The CCCH can include the following: (1) *paging channel* (PCH), which is a down channel used to page MSs; (2) *random access channel* (RACH), which is an uplink channel used for request assignment of a DCCH; and (3) *access grant channel* (AGCH), which is a downlink channel used to assign a MS to a specific DCCH.

A DCCH is a point-to-point, directional control channel. Two types of DCCHs are used: (1) *stand alone dedicated control channel* and (2) *associated control channel*

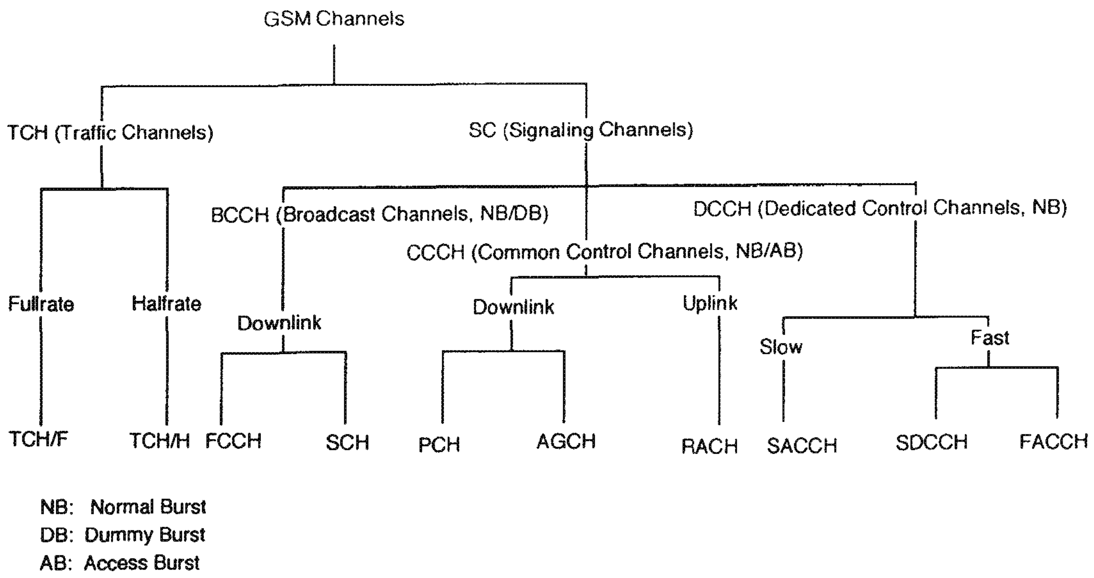


Figure 3.4 Logical channels in GSM.

(ACCH). Stand alone SDCCH is a DCCH whose allocation is not linked to the allocation of a TCH. This channel is used before the MS is assigned a TCH. The SDCCH is used to provide authentication to MS and for location updates and assignment to TCHs. A DCCH whose allocation is linked to the allocation of a TCH has ACCHs (that is, FACCH and SACCH). A FACCH or burst stealing is a DCCH obtained by preemptive dynamic multiplexing on a TCH. A SAACH, also known as a continuous data stream, is allocated together with a TCH or a SDCCH. We shall now provide details of each of these three groups of control channels.

3.2.3.1 Broadcast Control Channel

The BCCH provides general information on a per-BTS basis (cell-specific information) including information necessary for the MS to register in the system. After initially accessing the mobile, the BS calculates the required MS power level and sends a set of power commands on this channel. Other information sent over this channel includes country code, network code, local area code, PLMN code, RF channels used within the cell where the mobile is located, surrounding cells, hopping sequence number, mobile RF channel number for allocation, cell selection parameters, and RACH description. One of the important messages on a BCCH channel is CCCH_CONF, which indicates the organization of the CCCHs. From this parameter, the number of CCCHs (BS_CC_CHANS), indicating whether or not CCCHs are combined with four SDCCHs and four SACCHs on to the same physical channel called BS_CCCH_SDCCH_COMB = true or false, are derived as shown in Table 3.1.

Similarly, the 3-bit message BS_AG_BLKS_RES represents the number of blocks on each CCCH reserved for access grant messages. This channel is used to downlink point-to-multipoint communication and is unidirectional; there is no corresponding uplink. The signal strength of this channel is continuously measured by all mobiles, which may seek a handover from its present cell. Thus, it is always transmitted on a designated RF carrier (the "BCCH carrier") using timeslot 0, denoted as C0T0. This channel is never kept idle—either the relevant messages are sent or a dummy burst is sent. Other channels that belong to this group are the FCCH and SCH.

Table 3.1
CCCH Configuration Message Structure

CCCH_CONF	*BS_CC_CHANS*	*BS_CCCH_SDCCH_COMB*
000	1	false
001	1	true
010	2	false
100	3	false
110	4	false

The FCCH carries information for frequency correction of the MS downlink. It is required for the correct operation of a radio subsystem. Similar, to the BCCH, the channel is also for point-to-multipoint communication. This will allow an MS to accurately tune to a BS. FCCH sends all zeros in its burst to represent an unmodulated carrier, which we shall discuss in the next section.

The SCH carries information for the frame synchronization (TDMA-frame number) of the MS and the identification of a BTS. Similar to FCCH, this is also required for the correct operation of a mobile. The SCH channel carries a 64-bit binary sequence that is a priori known to the mobile. By correlating these bits with the internally stored 64 bits, MS achieves the exact timing (timing synchronization) with respect to a GSM frame. Specifically, the synchronization channel contains two encoded parameters: (1) *BTS identification code* (BSIC) and (2) *reduced TDMA frame number* (RFN).

The BSIC consists of six bits, out of which three bits represent the PLMN color code with a range from 0 to 7, and the other three represent BS color code with a range from 0 to 7.

The RFN is 19-bits long and consists of

T1(11 bits)	$= FN \text{ div}(26 \times 51)$	Range from 0 to 2,047
T2(5 bits)	$= FN \text{ mod}(26)$	Range 0 to 25
T3(3 bits)	$= (FN \text{ mod}(51) - 1) \text{ div}(10)$	Range 0 to 4

where FN represents the TDMA frame number. The layout of BSIC and RFN within the message part of the synchronization sequence is shown in Figure 3.5. SCH, FACCH, and BCCH channels cannot be frequency hopped, as these channels carry synchronization and system-related information whose exact location must be know to mobile.

In the BSIC, the channel is once again in the downlink direction only and is used for point-to-multipoint communication.

3.2.3.2 *Common Control Channels*

A CCCH is a point-to-multipoint bidirectional control channel and is primarily intended to carry signaling information necessary for access management functions (e.g., allocation of dedicated control channel). CCCH includes: (1) a PCH, which

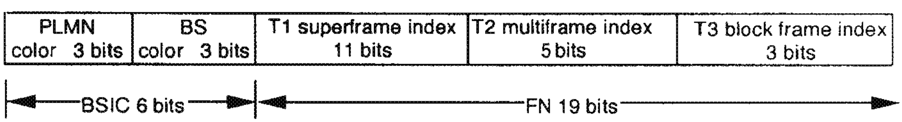


Figure 3.5 SCH message format.

is used to page (search) the MS in the downlink direction; and (2) a RACH, which is used by MS to request allocation of an SDCCH either as a page response from MS or call origination/registration from the MS. This is an uplink channel and operates in point-to-point mode (from MS to BTS). The channel operates on slotted Aloha Protocol and thus the contention possibility exists. If the mobile's request through this channel is not answered within a specified time, the MS assumes that a collision has occurred and repeats the request. Mobile must allow a random delay before reinitiating the request to avoid repeated collision.

The AGCH is used to allocate an SDCCH or a TCH directly to an MS. This channel is in the downlink direction and operates in point-to-point mode. A combined paging and access grant channel is designated as PAGCH, although the GSM specifications refer to PAGCH as two separate channels.

3.2.3.3 Dedicated Control Channels

DCCHs consist of a SDCCH and the ACCH. The SDCCH is used for system signaling during idle periods and call setup before allocating a TCH. For example, MS registration, authentication, and location update takes place through this channel. When a TCH is assigned to the MS, this channel is released. It uses 1/8 rate TCH (TCH/8); that is, its data rate is one-eighth of the full rate speech channel. This is achieved by transmitting data over this channel once every eighth frame. The channel is used for both up/downlink and is meant for point-to-point usage.

As stated, the SACCH can be linked to a TCH or an SDCCH. It is a continuous data channel carrying information, such as measurement reports, from the mobile of received signal strength for a serving cell as well as adjacent cells. This is a necessary channel for the mobile-assisted handover function. The channel is also used for power regulation of the MS and time alignment and is meant for both the up and downlink. It is used for point-to-point communication between mobile and BS.

A FACCH is associated to a TCH. FACCH works in a stealing mode. This means that if suddenly during a speech transmission it is necessary to exchange signaling information with the system at a rate much higher than the SACCH can handle, then 20-ms speech (data) bursts are stolen for signaling purposes. This is the case at handover. The interruption of speech will not be heard by the user since it lasts only for 20 ms and cannot be sensed by human ears. We shall now take up details of how the data is actually arranged within a physical channel for the logical speech and control channels.

3.2.4 Structure of a TDMA Slot With a Frame

There are five different kinds of bursts in the GSM system.

- Normal burst;
- Synchronization burst;

- Frequency correction burst;
- Access burst;
- Dummy burst.

3.2.4.1 *Normal Burst*

This burst is used to carry information on the TCH and on control channels, except for RACH, SCH, and FCCH, and is shown in Figure 3.6(a). Burst is divided into 156.25 bits. The first bit in the slot is numbered 0, and the last (1/4) bit period is numbered 156. The lowest bit number is transmitted first. The encrypted bits are 57 bits of data or speech plus one bit "stealing flag" indicating whether the burst was stolen for FACCH signaling or not. The training sequence is a known 26-bit pattern used by the equalizer to create a channel model. The reason why the training sequence is placed in the middle is that the channel is constantly changing. By having it there, the chances are better that the channel is not too different when it affects the training sequence compared to when the information bits were affected. If we put the training sequence at the beginning of a burst, the channel model we create might not be valid for the bits at the end of a burst. There are eight training sequences as shown in Table 3.2. The 26-bit equalization patterns are determined at the time of call setup.

The *tail bits* (TB) always equal (0,0,0), which has bit location from 0 to 2 and also from 145 to 147. They help the equalizer know the start and stop bit pattern; that is, the algorithm used in the equalizer needs a certain start/stop point. The *guard period* (bits) (GP) is empty space. Since we have a maximum of eight users per carrier, using different time slots, we must make sure that they do not overlap each other during the transmission. To synchronize the bursts with exact accuracy (with no GP) is not easy to do in practice since the mobiles are moving during the call and causing the bursts from different mobiles to "slip" a little (this can be caused by different delays, which in turn are caused by different locations of users within a cell) compared to each other. Thus, the 8.25 bits that correspond to about 30.46 μs (8.25 × 3.693) is allowed to protect the overlapping of messages at the BS. The GP also allows the transmitter to ramp-up and ramp-down within limits specified by the GSM recommendations.

3.2.4.2 *Synchronization Burst*

This burst is used for time synchronization of the mobile. It contains a long synchronization sequence (64-bits long). The training sequence states are: (BN42, BN43, . . ., BN105) = (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1). The encrypted 78 bits carry information of the TDMA frame number

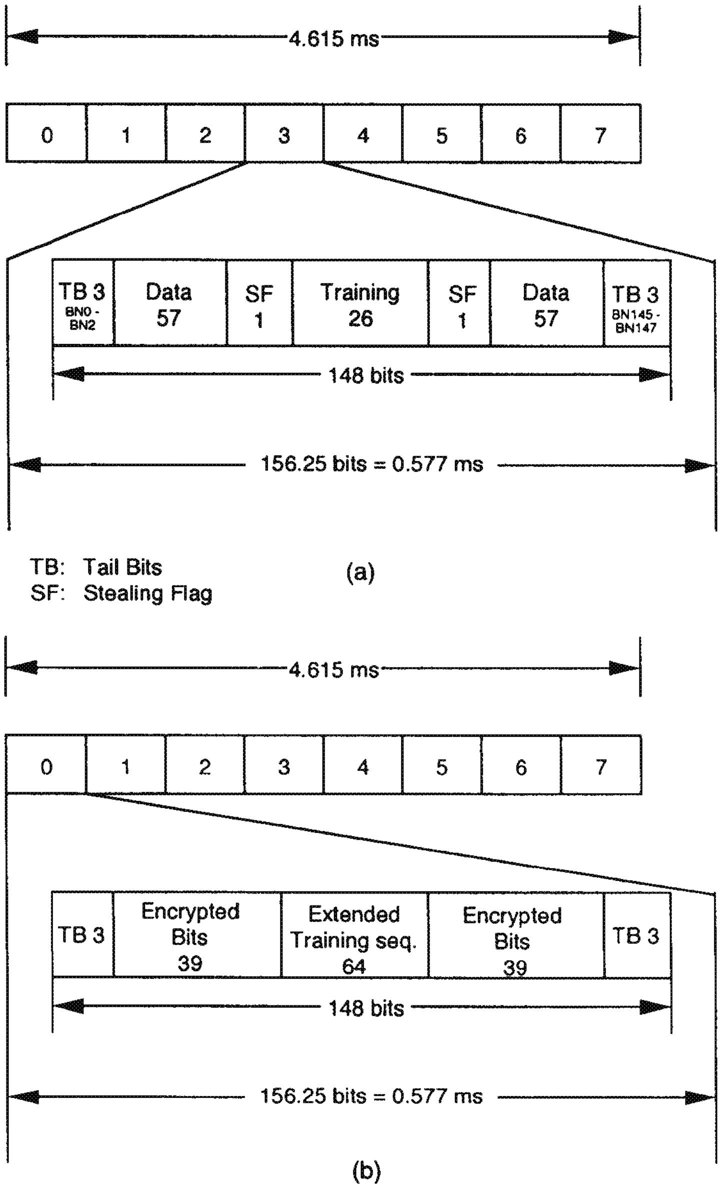


Figure 3.6 (a) Normal burst, (b) synchronization burst, (c) frequency correction burst, (d) access burst, and (e) dummy burst.

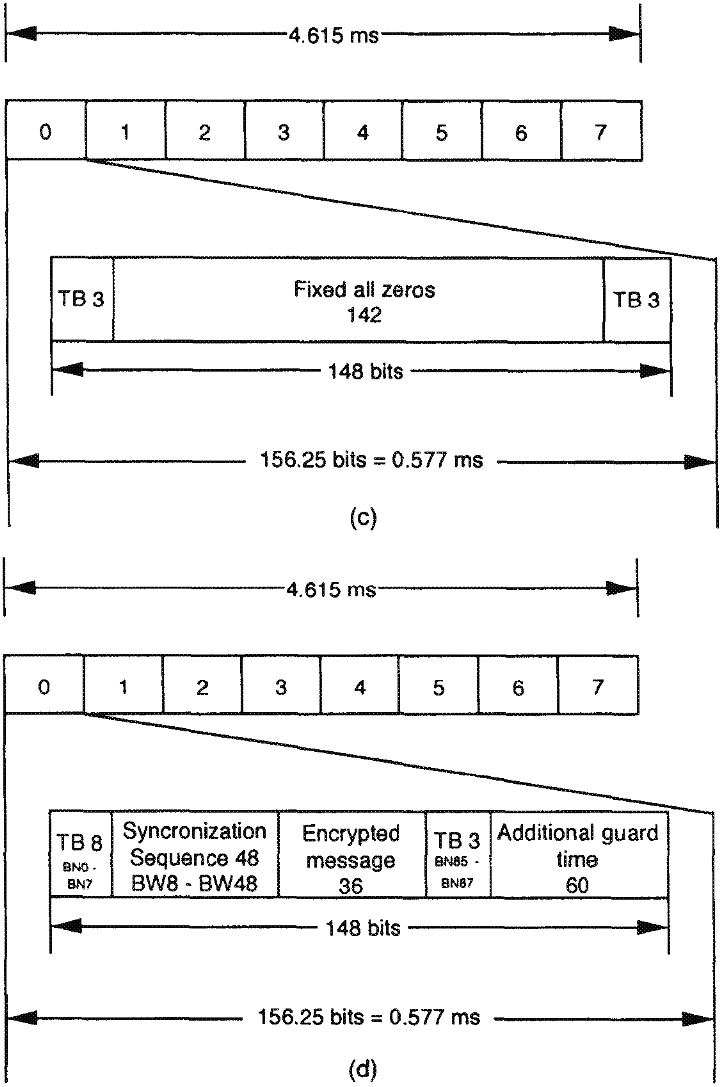


Figure 3.6 (continued).

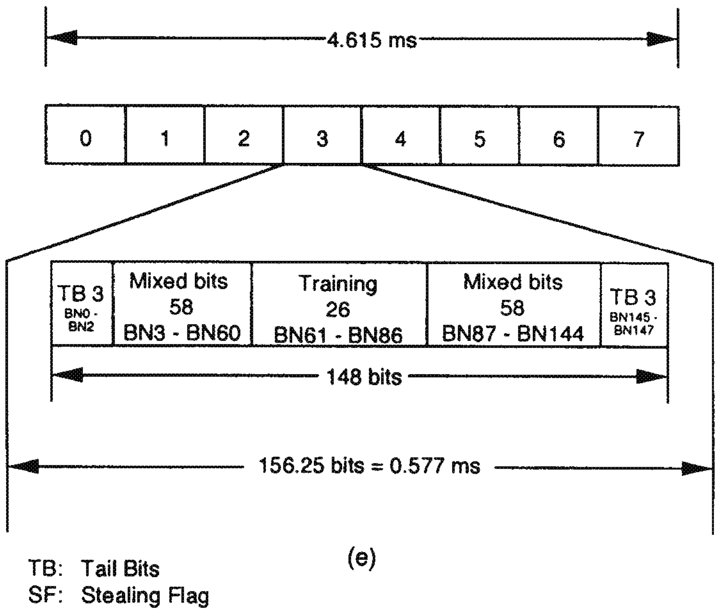


Figure 3.6 (continued).

Table 3.2
Normal Burst

Code Number	*Training Sequence Code (TSC) Sequence of 26 bits*
0	00100101110000100010010111
1	00101101110111100010110111
2	01000011101110100100001110
3	01000111101101000100011110
4	00011010111001000001101011
5	01001110101100000100111010
6	10100111110110001010011111
7	11101111000100101110111100

along with the BSIC, as discussed in the previous section. It is broadcast together with the frequency correction burst. These bursts are named as SCH and shown in Figure 3.6(b). The TDMA frame is broadcast over a SCH, as discussed in Section 3.3, in order to protect user information against eavesdropping, which is accomplished by ciphering the information before transmitting it. The algorithm that calculates the ciphering key uses a TDMA frame number as one of the input parameters, and

therefore, every frame must have a frame number. The numbering scheme is cyclic with a period of 3.5 hr (2715648 TDMA frames). An FN is encoded in 19 bits before channel encoding and is shown in Figure 3.5. Also, by knowing the TDMA frame number, the mobile will know what kind of logical channel is being transmitted on the control channel TS0. BSIC is also used by the mobile to check the identity of the BTS when making signal strength measurements (to prevent measurements on cochannel cells).

3.2.4.3 Frequency Correction Burst

This burst is used for frequency synchronization of the mobile. It is equivalent to an unmodulated carrier with a specific frequency offset. The repetitions of these bursts are called FCCH. The fixed input bits are all zeros, causing the modulator to deliver an unmodulated carrier with an offset of 1,625/24 kHz above the nominal carrier frequency. Here the TB and guard bits are the same as in normal burst. A frequency correction burst is shown in Figure 3.6(c).

3.2.4.4 Access Burst

This burst is used for random access and has a longer GP (68.25 bits or 252 μs) to protect for burst transmission from a mobile that does not know the timing advance when it first accesses the system. This allows for a distance of 35 Km from base to mobile. In case the mobile is far away from the BTS, the initial burst will arrive late since there is no timing advance on the first burst. The delay must be shorter to prevent it from overlapping the burst in the adjacent timeslot following this. Figure 3.6(d) shows the layout of an access burst. Here the extended tail bits are defined as modulating bits with the following states: (BN0, BN1, . . . , BN7) = (0, 0, 1, 1, 1, 0 ,1, 0). The TB are (0, 0, 0), and they occupy the position (BN85, BN86, BN87). Similarly, synch bits occupy the position (BN8 through BN48).

3.2.4.5 Dummy Burst

This burst is sent from BTS on some occasions. It carries no information. The format is the same as for a normal burst. Figure 3.6(e) shows the layout of a dummy burst. Here the TB occupy positions (BN0, BN1, BN2) and (BN145, BN146, BN147) and are (0, 0, 0) in both instances. The training sequence bits occupy positions BN61 through BN86. The mixed bits are defined as modulating bits states as

(BN3, BN4, . . ., BN60) = (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0,
1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1,
0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)

(BN87, BN88, . . . , BN144) = (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)

In the next section we shall build upon this information by discussing different organizations of signaling channels.

3.2.5 Time Organization of Signaling Channels

In this section we shall discuss how different traffic and control channels are organized. For establishing end-to-end communication between mobile and PSTN, or between two mobiles, a large amount of data has to be exchanged between the mobile and the system before a speech channel can be assigned to the mobile. Data are exchanged between mobile and the system over different logical control channels. In this section the layout of different logical control channels will be covered. To accomplish this we shall consider the layout of the following channels [2,3].

- Full rate and half rate TCHs;
- Signaling channels (downlink only): (1) FCCH and SCH, where the mobile synchronizes its frequency and reads the TDMA frame number and the BSIC; (2) BCCH, through which the mobile reads the necessary general information about the system; and (3) PAGCH;
- Signaling channel (uplink only): RACH, through which the mobile requests service either in response to a paging or as an initial request to originate a call;
- Signaling channel (bidirectional): SACCH and FACH;
- Common channel allocation in a typical system: (1) basic case, and (2) small-capacity system.

3.2.5.1 Time Organization of Traffic Channel (Full and Half Rate)

As stated, the TCH/F carries information (encoded speech or data) at the gross rate of 22.8 Kbps. The time organization of TCH is shown in Figures 3.7(a). A TACH/F contains TCH/F and SACCH. Eight different types of TACH/F can be defined based on their phase modulo 8 (TN_0 to TN_7). SCH channel occupies the 13th frame. The 26th frame is kept idle for future use.

A half rate TCH carries information (encoded speech or data) at a gross rate of 11.4 Kbps. The raw data rate is 7 Kbps for speech or data rates of 6 Kbps or